REMARKS/ARGUMENTS

Applicant would first like to express sincere appreciation to the Examiner for the courtesy extended to Applicant's representatives during the telephone interview of June 24, 2008 and the considerable time afforded to Applicant's representatives in attempting to resolve outstanding issues pertaining to the claims presented in the supplemental amendment filed in response to the August 24, 2007 Office Action.

In response to the telephone interview, Applicant is submitting this second supplemental amendment for the purpose of clarifying certain issues discussed during the telephone interview and for the purpose of having the claims distinguish even more clearly over the cited prior art and over additional patent references noted by the Examiner as possibly being relevant to Applicant's claims, and now placing the application in better form for allowance.

During the telephone interview Examiner indicated that rewriting dependent claim 20 in independent form would place that claim in much better condition for allowance.
Therefore, newly presented Claim 35 incorporates the limitations of Claim 15 and dependent Claim 20 in addition to intervening dependent claims in a manner which eliminates noted redundancies contained in such dependent claims.

Claims 15 and 20-35 are now active in the application after this amendment;
Claims 16-18 are newly cancelled without prejudice by this amendment because the more important limitations have now been incorporated into Claim 15, and dependent Claim 20, and also in Claim 35.

It is noted that after the telephone meeting Applicant identified that some of the prior art references discussed were cited of record in Continuation Patent Application number 11/802,759.

Comments on Claim 15 amendments:

The changes to claim 15, almost all of which were discussed during the telephone interview of June 24, 2008 with Examiner Colin, were made for the purpose of making the claim more understandable and for clarifying certain phrases contained in the claim.

The phrase "via a dedicated bus" describing an input / output module was replaced with the phrase "through a bus providing direct access by the encryption circuit to host computer system memory" because it is more consistent with the FIG. 1 of the Drawing.

The portion of the claim describing the "input / output module microcontroller and memory" has been amended to recite "the input/output module comprising a microcontroller and a microcontroller control memory, the microcontroller control memory providing storage for program control of the microcontroller". This clarifies the function of the microcontroller and its control mechanism consistent with the description in paragraphs [0027 to 0034] and in particular paragraphs [0029, 0030, and 0034] which describe the function of the flash memory, SRAM memory and well known equivalent technology such as DRAM memory. It will be appreciated that the distinction between specific types of memory utilized by the microcontroller are not pertinent to the invention, only the functionality of the memory is relevant.

The phrase "coupled to the input/output module" describing the encryption module has been deleted since it could be considered somewhat misdescriptive because the encryption module is operatively coupled to the input / output module only through the isolation means. Thus, Applicant believes that the claim is made clearer by describing the connection with regards to the descriptive portion of the claim relating to the isolation means (see below).

The isolation means is now defined in this claim as comprising a "dual port memory" described in illustrated embodiment of the invention and recited in dependent claim 16.

The claim has been further amended by defining the parallelism achieved by the invention and is specifically claimed by describing the parallelism between the input / output module and the encryption module. As discussed in telephone interview with the Examiner on June 24, this aspect of the present invention is adequately described in paragraphs [0013, 0014 and 0031] of the published continuation application 11/802,759 which contains the identical description as the present application. Some discussion of this same point is also presented in Applicant's prior supplemental amendment.

Arguments for allowance of amended claim 15:

The prosecution history has extensive arguments concerning referenced prior art. This discussion below is meant to be a very brief summary of the most recent points, presented briefly for convenience of the Examiner. The following discussion also comments on other references not specifically applied to Applicant's claims but referred to by the Examiner during the telephone interview of June 24, as noted above.

Brief Comments Concerning the DYKE Patent Reference indirectly referenced in the August 24, 2007 Office Action and discussed in the Telephone Interview of June 24, 2008 –

In the PRE-APPEAL BRIEF REQUEST FOR REVIEW filed May 24, 2007, there is presented arguments as to why DYKE does not teach or suggest the Applicant's invention, and also a discussion of a cited secondary reference corresponding to an IBM Technical Disclosure Bulletin.

The Applicant respectfully submits that these arguments are still applicable with claim 15 in its currently amended form. The key point made in the Pre-Appeal Brief Request is that DYKE does not teach or suggest an Input/ Output module as defined in claim 15. This is shown most clearly in FIG. 1 of DYKE, as discussed in the Brief. In particular it is noted that the Dual Port RAM of DYKE is connected directly to the host computer, and thus is directly readable and writable from the host computer, thus no isolation or protection is provided. CPU 25 does not function as an Input/Output controller since it is on the opposite side of the dual port RAM, and Host Computer 12 is the Host System Central Processor so it does not function as the Input/Output Module's microcontroller as defined in claim 15. More detailed arguments are contained in the Brief.

In the telephone interview of June 24, 2008, it was pointed out that the claim 15 under review in the Pre-Appeal Brief included the phrase "the input/output module further including a flash memory and a static random access memory ..." and that deleting this phrase from the claim removed a significant limitation. The same reason is also discussed in the Office Action of August 24, 2007. Applicant submits that just because the flash memory and static memory elements were subsequently omitted from claim 15 should not change the conclusion that claim 15 is patentable over DYKE for the reasons given in the Pre-Appeal filed May 24, 2007 since those elements were not key to the argument. In response to the Examiner's comments during the telephone interview of June 24, 2008 Applicants this supplemental amendment now includes limitations similar to those contained in the version of claim 15 which was subject of the Pre-Appeal Brief.

Specifically, it now includes the phrase "the input/output module comprising a microcontroller and a microcontroller control memory, the microcontroller control memory providing storage for program control of the microcontroller;" This phrase more accurately describes the Input/Output module as depicted in FIG. 1 of the Drawing, and as described in paragraphs [0027 to 0034] of the original specification.

It is also noted that the amendment to claim 15 in this supplemental amendment pertaining to the connection of the encryption circuit to the host system memory further clarifies the patentable differences between claim 15 and teachings of DYKE. Thus the currently proposed amendment to claim 15 pertaining to the connection of the encryption circuit to the host system memory is now more descriptive and even further clarifies the patentable differences between claim 15 and teachings of DYKE.

Brief Comments Concerning the RUSS Patent cited and applied in August 24, 2007 Office Action –

Detailed arguments concerning RUSS are presented in the Supplemental Amendment with remarks filed February 8, 2008. RUSS teaches the architecture of a front-end processor with purposes and architecture distinctly different than the Applicant's invention as defined in amended Claim 15.

RUSS does not describe "an input/output module coupled to the host computer system through a dedicated bus". The MPU of RUSS is not provided with a dedicated bus for access to the host system. The DBUS and UBUS of RUSS are both utilized for several other operations relating to encryption and decryption, and general data movement.

This sharing of functionality on the DBUS in RUSS further precludes the parallelism which is a part of an illustrated embodiment of the Applicant's invention as defined in the currently amended Claim 15. The architecture of RUSS specifically does not allow parallelism between data exchange on the host system bus, and data exchange for encryption and decryption because the data movement for both of these operations utilizes the "DBUS" and so it cannot be done in parallel. Further, the use of a memory which contains arbitration logic in RUSS for arbitrating memory access requests on a priority basis intentionally precludes concurrent or parallel access to the memory by more than one source.

RUSS is silent about "storage of sensitive information". As discussed in Applicant's previous supplemental amendment, RUSS teaches providing encryption as an option (see column 12 of RUSS) and therefore, there would be no reason to address the storage of sensitive data. Moreover, in RUSS, the host system initiates block transfers of

data via interrupts and supplies required parameters to the front end processor. Thus it appears that the supplied parameters would have to include encryption parameters and this would imply that the host system would have access to sensitive information in order to supply those parameters.

Brief Comments Concerning BAKHLE patent reference cited and applied in the August 24, 2007 Office Action –

BAKHLE is provided by the Examiner as a secondary reference with regards to Claim 15 and others. BAKHLE describes the architecture of a cryptographic circuit for providing "simultaneous ciphering and hashing".

As discussed in the previous Supplementary Amendment, BAKHLE does not describe or suggest the type of parallelism provided by Applicant's invention as defined in amended Claim 15. The parallelism of BAKHLE is between a cryptographic operation and a hashing operation which both operate on the same data to complete encryption of a single block. This is not the parallelism of data movement which is one subject of the Applicant's claimed invention.

BAKHLE also does not describe an "input/output module comprising a microcontroller and a microcontroller control memory" that is utilized in the manner defined in amended claim 15 consistent with the teachings of Applicant's invention. The cryptographic device of BAKHLE in FIG. 1 and shown in more detail in FIG. 2 illustrates a Management Processor 142 and a DMA unit 149 which controls the Bulk Cryptographic Cluster (BCC) 148. The Management Processor provides for control of the input / output from the BCC, but does not teach that the Management Processor operates as an independent input/output controller. As illustrated in BAKHLE FIG. 8, data is loaded into the IN buffer, and no data is written out from the OUT buffer until the encryption operation is "DONE". The Management Processor does not start loading data for any further encryption operation until the present encryption operation is "done". BAKHLE is limited to this approach because the encryption (ciphering) of BAKHLE is done in parallel with a hashing operation which may take a different number of cycles. Therefore, a new block for encryption cannot be accessed until both operations are completed. This is described in BAKHLE in the Summary of the Invention Column 2, lines 10-13. "The security enhancement unit ensures that the cipher unit and hash unit do not accept a next block of data (i.e. new data) until both units have completed processing the current block of data". The Management Processor also is responsible for providing data to the BCC (BAKHLE, Column 5, Line 34-35), and the decryption software executes on the Management Processor (Column 5, Line 44). This further precludes its

functioning simultaneously or independently as an Input/Output processor and in achieving the higher performance and parallelism of data movement as in the Applicant's invention defined in amended Claim 15.

Considerations in Combining References:

Even if an attempt were made to combine the teachings of BAKHLE with the teachings of DYKE or RUSS in some manner, it is unpredictable as to what form the resulting combination would take due to the differences in architectures between the systems described in DYKE, RUSS and BAKHLE.

RUSS teaches parallelism and performance improvement using multiple buses surrounding a single port RAM or DRAM which provides priority arbitration for memory access by multiple bus sources/devices. This teaches away from the approach of utilizing a multiple port RAM as in BAKHLE for carrying out a single encryption operation on a block of data at a time.

BAKHLE teaches parallelism of hashing and ciphering, but with a standard architecture providing no improvement in performance for just encryption or decryption and teaches explicit restriction against parallelism in processing of different blocks of data in order to achieve simultaneous hashing and ciphering.

DYKE teaches parallelism of encryption and decryption with data movement into a dual port RAM 14, but there is no Input/Output module provided so the work of moving data must be done by the Host Computer 12 which is a significant disadvantage solved by the Applicant's claimed invention which provides an independent Input/Output module for movement of data into the encryption circuit card, thus freeing up the Host Computer to do other work.

DYKE, RUSS, and BAKHLE all have microcontrollers which control in some way input/output from their circuitry. However:

in DYKE the host system does its own writing into a dual port RAM 14 which is connected directly to the host system bus 44 and the microcontroller 26 is in control of the encryption circuitry 28;

in RUSS, the microcontroller MPU 50 is not provided with a dedicated connection (DBUS or UBUS) and must connect its CBUS to the DBUS in order to perform I/O, which cannot be done in parallel with operations performed by Encryption 62 which also utilizes DBUS; and

in BAKHLE, the microcontroller Management Processor 142 is an overall control processor of both I/O and ciphering and is prevented by its architecture from performing

I/O operations for providing the data to be encrypted or decrypted while it is performing any processing operations for ciphering or hashing.
Thus, Applicant submits that none of these references provides or describes an Input/Output module with a microcontroller connected as described in the Claims defining the Applicant's invention.

Other References:

The Examiner during the telephone interview of June 24, 2008 mentioned two additional patents that had been briefly analyzed as relating to the Applicant's invention. These were Patent Number 5,333,198 Houlberg et. al. titled "Digital Interface Circuit", and Patent Number 5,621,800 Weng et. al. titled "Integrated Circuit that Performs Multiple Communication Tasks". These two references were examined briefly by Applicants for consideration as to their relevancy to Applicant's claimed invention.

HOULBERG describes an invention which is a protocol convertor for allowing a first and second device to communicate where one operates serially and the second is by parallel communications. The first device may be an encryption unit. The protocol converter includes a dual port memory. The details of the encryption unit are not provided, and the architecture and purpose of the circuits are significantly different than the Applicant's invention so it does not appear to the Applicants to be relative prior art. As seen from the claims, HOULBERG is related entirely to serial / parallel communication, and not improvement of encryption or improvement in the performance of encryption hardware.

WENG presents an integrated circuit that includes memory and a central processor which executes a codec algorithm. The architecture is somewhat similar to that of BAKHLE in that a Signal Processor which includes a Central Processing Unit is connected almost directly to an external Digital Data bus 46 through a Data Port 38. The Digital Data bus 46 can be connected to a personal computer 42. It is not apparent that there is any form of input / output module or input/output microcontroller, nor any means of isolation. In addition, as for HOULBERG, the invention is intended for application in the communications field and the data is streamed through the unit to an RF interface 16, so the purpose, the data movement and the architecture of the WENG circuitry are significantly different than that of the Applicant's claimed invention.

Applicants therefore submit that due to the significant technology and architectural differences, and different purposes for application of these inventions, that there is no suggestion to combine any teachings or aspects of these inventions with other

prior art to achieve the advantages, purposes or the architectural structure of the Applicant's invention as defined in the amended claims.

Conclusion:

In view of the above arguments and clarifying amendments, Applicants submit that amended claims 15-18 and 20-34 and/or new independent claim 35 should be deemed patentable over the cited prior art. A notice to this effect is respectfully solicited. Applicants ask the Examiner to contact Applicant's representative to further discuss any grounds for rejecting Applicants claims if necessary before acting on this amendment. Also, if any questions or issues should arise with respect to this amendment or the allowability of this application, the Examiner is urged to call Applicants' representative at the number indicated herein.

Additionally, if the Examiner feels that further discussion will further advance the prosecution of this application, the Examiner is also urged to call as suggested herein.

Applicants further specify that the preceding arguments and discussion are for purposes of discussing an illustrated embodiment of the Applicant's invention and should not be construed as limiting. The bounds of the claimed invention are as defined in Applicant's claims as interpreted in light of the specification.

Respectfully submitted,

Russell W. Guenthner, Ph.D.
Reg. # 54,140
Office Phone Number: 602 862-5479